CORESTREAM

22.08.2023

Information Security Policy v1.5

Document Control

Any change to the Information Security policy is detailed below. The policy is stored within SharePoint and so a version history and audit log of who made changes (and when they were made) is automatically maintained.

The Information Security policy document can be fully revised and re-issued at the discretion of the Senior Leadership Team.

The Information Security policy will be reviewed annually.

NB: The document control information is used to supplement versioning within CoreStream Internal where this document is stored.

Issue	Amendment	Date	Initials
0.1	Initial draft of Information Security Policy	08/07/16	SL
0.2	Updated to include the changes to physical security controls, in light of CoreStream's office move in early 2017.	22/08/17	SL
0.3	Updated to include details of employee PC security settings	11/10/17	ME
0.4	Updates made to include processes on the handling of client data	15/01/18	ME
0.5	Reviewed ahead of annual audit, and no changes deemed necessary.	13/08/18	SL
0.6	Updated the scope to clarify that it applies to office workers and remote workers	07/01/19	SL
0.7	Updated to reflect the Information Security Officer being Matt Eddolls.	01/05/19	SL
0.8	Updated policy on automatic locking of laptops.	06/05/19	SL
0.9	Reviewed ahead of annual audit, and no changes deemed necessary.	14/08/19	SL
1.0	Reviewed and added a new section on Audit Logging.	18/03/20	SL
1.1	Reviewed and no changes deemed necessary.	14/04/21	SL
1.2	Reviewed and no changes deemed necessary.	12/07/22	SL
1.3	Reviewed and updated with Sophos anti-virus software and our updated URL for the Incident Management system	22/06/23	SL

1.4	Removed clause allowing recreational use of laptops by immediate household members	10/07/23	ME
1.5	Removed all the detailed policy procedures and controls to our Acceptable and Fair Use Policy, and aligned our policy objectives with ISMS objectives (on the recommendation of our BAB auditor)	22/08/23	SL

Table of Contents

1. Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of CoreStream. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for CoreStream to recover.

CoreStream is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which CoreStream is responsible.

2. Purpose

The primary purposes of this policy are to:

1. Ensure the protection of all CoreStream information systems (including but not limited to all computers, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.
2. Make certain that users are aware of and comply with all items in this policy.
3. Provide a safe and secure information systems working environment for staff and any other authorised users.
4. Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
5. Protect CoreStream from liability or damage through the misuse of its IT facilities.
6. Respond to feedback and update as appropriate, initiating a cycle of continuous improvement.

3. Scope

The scope of this policy applies to:

- All CoreStream staff and contractors (including office workers and remote workers).
- Third parties who interact with information held by CoreStream and the information systems used to store and process it.
- Any systems or data attached to the CoreStream data, systems managed by CoreStream, mobile devices used to connect to CoreStream networks, data over which CoreStream holds the intellectual property rights and data over which CoreStream is the data owner or data custodian.

4. Policy

4.1 Policy Objectives

The objectives of this policy with regards to the protection of information system resources against unauthorised access are as follows:

1. CoreStream will deliver its services within a secure and reliable environment.
   - This will be measured via system uptime (availability), monitoring of any failures in our backups (integrity) and the number of complaints received or information breaches (confidentiality)
2. CoreStream will operate as a digital paperless organisation.
   - This will be measured by the volume of electronic and hard copies of documents being held by CoreStream.
3. CoreStream will conduct quarterly risk assessments to ensure that the risk to information in the care of CoreStream is minimised or eliminated.
   - This will be measured via periodic risk assessments and reviews / updates to the Risk Register and mitigating actions.
4. CoreStream will minimise the threat of accidental, unauthorised or inappropriate access to critical or sensitive electronic information owned by CoreStream or temporarily entrusted to it by applying a proportionate level of encryption control.
   - This will be measured by the cryptographic controls in place for CoreStream, and the number of data breaches.

4.2 Policy Overview

CoreStream’s information system resources are important business assets that are vulnerable to access by unauthorised individuals or unauthorised remote electronic processes. Sufficient precautions are required to prevent unwanted access by applying a level of encryption to critical and sensitive data, which is proportionate to the business risk. Users should be made aware of the dangers of unauthorised access, and managers should, where appropriate, introduce encryption controls to prevent such access.

For a detailed overview of our information security processes, procedures and controls please refer to the *Acceptable and Fair Use Policy*.

For more information please contact:

SOPHIE LIS

DIRECTOR OF COMPLIANCE AND
INFORMATION GOVERNANCE

+44(0)7841 515862

SOPHIE.LIS@CORESTREAM.CO.UK